Formalna verifikacija programske potpore - FVPP

Sveučilište u Zagrebu
Fakultet elektrotehnike i računarstva
Diplomski studij, 2. semestar
Ak. god. 2022./2023.

Nositelj predmeta:
izv. prof. dr. sc. Alan Jović, ZEMRIS, soba D-340, *alan.jovic@fer.hr*

Asistent:
Igor Stančin, mag. ing., ZEMRIS, soba D-335, *igor.stancin@fer.hr*

Web stranice predmeta: **https://www.fer.unizg.hr/predmet/fvpp**

FVPP plan nastave (po tjednima)

1. Nastavna cjelina: pregled područja, logike i alati za formalnu verifikaciju

1. tjedan: Pregled područja formalne verifikacije

2. tjedan: Teorijske osnove provjere modela. Propozicijska i predikatna logika

3. tjedan: Vremenska logika CTL. Formalna verifikacija kritičnih programskih dijelova – **NuSMV**

4. tjedan: Vremenske logike LTL, CTL*, eksplicitno izračunavanje skupova stanja

5. tjedan: Formalna verifikacija stvarnih programa u jeziku Java – **Java PathFinder**

6. tjedan: Priprema za međuispit.

7. tjedan: -- (gubimo zbog praznika)

8a. – 8b. tjedan: ---- međuispit

2. Nastavna cjelina: algoritmi za formalnu verifikaciju i simboličko izvršavanje programa

9. tjedan: -- (gubimo zbog praznika)

10. tjedan: Predstavljanje Booleovih funkcija, BDD-ovi, ITE-algoritam, primjena

11. tjedan: Problem zadovoljivosti. Poznati SAT-rješavači – **Izrada SAT-rješavača**

12. tjedan: Problem ispitivanja zadovoljivosti u teoriji (SMT). Simboličko izvršavanje programa.

13. tjedan: Hoareova logika i Dafny || CPROVER i JBMC

14. tjedan: Priprema za završni ispit

15. tjedan: ------ završni ispit

Formalna verifikacija programske potpore

Nastavne obveze FVPP (5 ECTS bodova):

- **Predavanja** (3 sata tjedno, 7+6 tjedana)
- **Domaće zadaće** (3), obavezne, kod kuće rješavanje
- **Međuispit** (1), bez ponavljanja, uživo
- **Završni ispit** (1), bez ponavljanja, uživo
- **Ispiti na rokovima**

Napomena: u slučaju značajne izmjene epidemioloških mjera ili drugih nepredvidljivih događaja moguće su izmjene načina izvođenja svih komponenti nastave. Studenti trebaju pratiti obavijesti na web stranicama predmeta.

Formalna verifikacija programske potpore

Predavanja:

- Ponedjeljkom od 9 do 12h u prostoriji A-301
- Prisutnost i aktivnost na predavanjima donose dodatne bodove (do 7 dodatnih bodova)
- Svi materijali (PDF-ovi slajdova, PDF-ovi *handoutsa*, dodatne poveznice, dodatni zadatci i sl.) bit će dostupni u sustavu Moodle
- Bilo kakve promjene od navedenog rasporeda bit će na vrijeme objavljene na web stranicama predmeta

Formalna verifikacija programske potpore

Ostvarivanje bodova tijekom kontinuirane provjere znanja:

- **Domaće zadaće** (3): 40 bodova. Potrebno je ostvariti barem **16 bodova (40%)**
- **Međuispit**: 30 bodova (nema praga, prva nastavna cjelina)
- **Završni ispit**: 30 bodova (nema praga, druga nastavna cjelina)
- Prag na ukupne rezultate međuispita i završnog ispita: **20** bodova (33%)
- Za prolaz predmeta potrebno je ukupno ostvariti barem **50** bodova
- Razdioba bodova prema pragovima **50 – 63 – 75 – 88** za ocjene 2 – 3 – 4 – 5

Formalna verifikacija programske potpore

Domaće zadaće – rješavanje:

- Domaće zadaće (3) rješavaju se kod kuće prema odgovarajućim strukturiranim uputama koje će biti dostupne na web stranicama predmeta tijekom semestra
- Domaće zadaće će se provjeravati u terminima laboratorijskih vježbi u određenim tjednima tijekom semestra
- Nadoknada **najviše jedne domaće zadaće** u dodatnom terminu na kraju semestra
- Provjera domaće zadaće mimo definiranih termina neće biti moguća i povlači za sobom pad predmeta u ovoj ak. godini
- Studentima koji ponavljaju predmet priznaju se domaće zadaće položene prošle godine

Formalna verifikacija programske potpore

Domaće zadaće i laboratoriji profili (samo za FER 2 program):

- **Bodovi iz domaćih zadaća čine bodove koje studenti unose u predmet "Laboratorij profila".**

  Zadaće ukupno nose **40 bodova**. Postotak uspješnosti na predmetu FVPP za Laboratorij profila je: $x/40 * 100$ (%), gdje je x broj ostvarenih bodova studenta na tri domaće zadaće.

  Postotak se dijeli s ***n***, gdje je ***n*** broj predmeta koji sudjeluju u pojedinom Laboratoriju profila (obično n=2).

- Napomena (1): Svaki Laboratorij profila samostalno određuje nužan postotak za prolaz kao i bodovne pragove za ocjenu.

Formalna verifikacija programske potpore

- **Ostvarivanje bodova na rokovima**

  - Najmanje **16** bodova iz domaćih zadaća
  - Ostvareni bodovi iz domaćih zadaća prenose se na ispitni rok (maksimalno 40 bodova).
  - **Pismeni ispit** na roku: **60 bodova**.
  - Ispit na roku (60 bodova) obuhvaća gradivo čitavog predmeta
  - Za prolaz predmeta potrebno je na ispitnom roku ostvariti barem **20** bodova (od 60, dakle 33%).
  - Za prolaz predmeta potrebno je ukupno ostvariti barem **50** bodova.
  - Razdioba ocjena je prema pragovima kontinuirane provjere.

Formalna verifikacija programske potpore

- 1. Domaća zadaća – tema:

Formalna verifikacija kritičnih programskih dijelova

U prvoj domaćoj zadaći potrebno je formalno verificirati upravljanje sustavom i interakciju **kritičnih dijelova programske potpore** uporabom sustava **NuSMV**.

Ulazni jezik u NuSMV je opis relacije prijelaza sustava pomoću Kripkeove strukture te definiranje provjere željenog obilježja u sintaksi vremenske logike CTL.

Nosi najviše **10** bodova

Vremenski okvir: 3. – 4. tjedan nastave (detaljnije u obavijesti o zadaći)

Formalna verifikacija programske potpore

- 2. Domaća zadaća – tema:

Formalna verifikacija programa pisanih u Javi

U drugoj domaćoj zadaći cilj je provjera modela programske potpore pisane u Javi uporabom sustava **Java PathFinder**. Studenti se na predavanju upoznaju s funkcioniranjem i strukturom sustava te s nekim proširenjima osnovnog sustava. Cilj domaće zadaće je pronalazak kvarova u programima pisanima u Javi postupkom provjere modela.

Nosi najviše **10** bodova

Vremenski okvir: 5. – 6. tjedan nastave (detaljnije u obavijesti o zadaći)

Formalna verifikacija programske potpore

- 3. Domaća zadaća – tema:

Izrada SAT-rješavača

Treća domaća zadaća donosi izradu programa za rješavanje problema zadovoljivosti Booleovih formula – SAT-rješavača. Studenti se na predavanju upoznaju s teorijom CDCL SAT-rješavača, a u domaćoj zadaći studenti trebaju izraditi vlastiti SAT-rješavač u jeziku po izboru (C, Python, Java) te ga vrednovati na javno dostupnom skupu problema.

Nosi najviše **20** bodova

Vremenski okvir: 11. – 14. tjedan (detaljnije u obavijesti o zadaći)

Formalna verifikacija programske potpore

- Literatura
  - **M. Huth, M. Ryan. Logic in Computer Science, Cambridge University Press, 2004.**
    - *ftp://ftp.cs.bham.ac.uk/pub/authors/M.D.Ryan/tmp/Anongporn/Ch1+3.pdf*
  - J. Rushby. A Rapid Introduction to Mathematical Logic, Appendix A, in: Formal Methods and the Certification of Critical Systems, Technical Report CSL-93-7, SRI International, 1993, str. 225-250. https://tinyurl.com/ztxvlxk
  - D. Kroening, O. Strichman, Decision Procedures: An Algorithmic Point of View, 2nd Ed., Springer, 2016.
  - M. Ben-Ari, Mathematical Logic for Computer Science, Springer, 2012
  - K. Schneider. Verification of Reactive Systems: Formal Methods and Algorithms, Springer-Verlag, 2010.
  - S. Demri, V. Goranko, M. Lange, Temporal Logics in Computer Science: Finite State Systems, Cambridge University Press, 2016.